DATALOCKER

DL4 FE ENCRYPTED DRIVE

FIPS 140-2 Level 3 Certified Encrypted Drives With Powerful Remote Management

SECURE TO THE CORE

The DL4 FE is a FIPS 140-2 Level 3 (Cert. #3972) Certified device built around a powerful AES 256-bit cryptographic hardware architecture that then adds layer after layer of security with automated policies that intelligently change its security posture based on its location, how it's being used, and the type of data being stored on it. The DL4 FE is a TAA compliant device that meets the strictest security requirements while offering large-capacity (up to 15.3 TB) and an easy-to-use touchscreen for setup and use. A powerful addition to the DataLocker line of securely managed solutions, the DL4 FE continues our proud tradition of providing Simply Secure™ solutions, plus it's backed by a limited 3-year warranty.

Powerful Encryption Right Out Of The Box

Everything you need to encrypt data is built into the FIPS 140-2 Level 3 and Common Criteria certified* DL4 FE. No drivers. No setup. Just iron-clad, hardware-based AES 256-bit encryption in an easy-to-use interface, which is further guarded by an army of automated security policies.

Never Risk Losing Your Data

Remote management policies with SafeConsole® lets admins remotely lock, erase or render devices unusable with remote device detonate, destroying all data in cases of attempted theft. SilentKill™ further gives users a special code to destroy the device's encrypted data in case of emergencies.

Ensure User Adoption With Easy-to-Use Touchscreen

A color touchscreen gives end-users quick access to secure data and allows them to customize their device. On-screen instructions make setup fast and easy. Randomized keypad layout with letters, numbers and special characters prevents surface analysis of fingerprints or prevents threat actors from guessing a repeated input pattern.

Remotely Manage & Audit Your Entire Fleet

All DL4 FE drives are remotely manageable with SafeConsole, giving admins the ability to remotely lock or wipe drives, reset passwords, view last-used locations, and see what data has been added, removed, or changed on the drive. Set device or group-specific policies for all the drives in your fleet.

*DL4 FE isin process to achieve Common Criteria cPP certification. The official listing as a Product under Evaluation by NIAP is expected in 2021.

THE DL4 FE

FIPS 140-2 LEVEL 3 CERTIFICATION
True device level 3 certification with a Common Criteria EAL5+ certified controller inside. Provides always-on hardware-based encryption. Dedicated AES 256-bit XTS mode crypto engine meets rigorous cryptographic standards and is more secure than software-based alternatives. Hardened internals and enclosure for increased physical security.

SILENTKILL™
Allow users under duress to destroy the device or the stored data without leaving traces by entering a special code (admin configurable).

FULLY MANAGEABLE DEVICE
Use DataLocker SafeConsole to manage individual and groups of devices using automated policies.

ADMIN POLICIES & USER DATA RECOVERY
Admins can set rigorous password policies (non-sequential, non-repeating special characters, minimum characters). Should users forget a password, admins can unlock the DL4 FE using the admin password. Admins can also recover the user's data by logging in with the admin password. The user will be forced to reset their password upon their next use.

BRUTE FORCE PASSWORD PROTECTION
When in use, admins can configure how many failed password attempts are needed before the device destroys its payload.

NOTHING TO INSTALL
All encryption, administration, and authentication performed on the DL4 FE unit. This means devices in standalone mode don't require a software agent; they work right out of the box.

THE DL4 FE MANAGED FEATURES

REMOTE DEVICE DETONATION
Lets admins functionally destroy the device and its data remotely to protect against data or encryption key theft (Admin configurable. Requires SafeConsole).

ON BOARD ANTI-MALWARE
Automatically scans files and quarantines/destroys bad apps/files based on policy settings (optional upgrade. Requires SafeConsole).

DATA GEOFENCING
SafeConsole uses geofencing, trusted networks, and ZoneBuilder to ensure a device changes its security posture based on its location (Admin configurable. Requires SafeConsole).

COMPREHENSIVE AUDIT CAPABILITIES
Have a complete record of file activity (including name changes on the device), password attempts, device locations and machines, device health, and policies in force (Admin configurable. Requires SafeConsole).

TECHNICAL SPECIFICATIONS

CAPACITIES
SSD: 1 TB, 2 TB, 4 TB, 7.6 TB, 15.3 TB

HDD: 500 GB, 1 TB, 2 TB

DIMENSIONS
L: 12.3 cm W: 7.7 cm
H: 2.1 cm

L: 4.8" W: 3" H: .82"

WEIGHT
.65/lbs / 294 grams and up

PHYSICAL SECURITY
Kensington Security Slot™

Hardened internals and enclosure

CRYPTOGRAPHIC PROCESS
FIPS 140-2 Level 3 Device Certified (#3972). Common Criteria cPP certification pending.

AES 256-bit XTS hardware encryption onboard.

Integrates a Common Criteria EAL 5+ certified secure microprocessor.

INTERFACE
USB-C on the device, compatible with USB 3.2, USB 2.0 (8 TB drives and under)

(USB-C to USB-A and USB-C to USB-C cables included)

TRANSFER SPEEDS
USB-C 3.2: 150 MB/s read, 100 MB/s write

USB 2.0: 40 Mb/s Read, 20 MB/s Write

STANDARDS AND CERTIFICATION
FIPS 140-2 Level 3
TAA Compliance
IP64 Certified
RoHS Compliant
FCC
CE

MANAGEMENT COMPATIBILITY
Microsoft Windows

OS COMPATIBILITY
Microsoft Windows, macOS®, Linux® or any machine that supports a USB mass storage device.

PART NUMBERS
DL4-500GB-FE
DL4-1TB-FE
DL4-2TB-FE
DL4-SSD-1TB-FE
DL4-SSD-2TB-FE
DL4-SSD-4TB-FE
DL4-SSD-7.6TB-FE
DL4-SSD-15.3TB-FE

DEVICE LANGUAGES
English, French, German, Spanish

WARRANTY
3-year limited warranty

TRUSTED BY

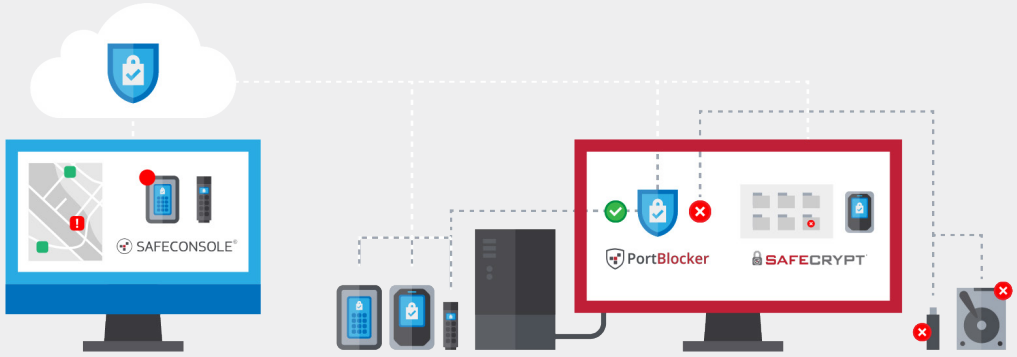
DATALOCKER®
SIMPLY SECURE

Get a Custom Demo

datalocker.com | sales@datalocker.com

THE COMPLETE DATALOCKER SOLUTION

The full DataLocker solution empowers workforces with secure mobile USB storage while giving admins the ability to monitor, audit, and manage devices remotely. From transport of sensitive data to updating remote machines, securing medical records, and more, DataLocker Solutions are a powerful way to fortify your most sensitive data.



SafeConsole - Remotely manage and audit secure drives

SafeConsole offers a cloud-based or on-prem dashboard where admins can manage and audit secure drives, manage virtual drives, and lock down USB ports from anywhere. If you're an admin looking for a way to secure hundreds of remote drives, SafeConsole is a superb option.

- Manage encrypted USBs, hard drives, and virtual drives
- Set policy rules like file-type restrictions and geographic boundaries
- Configure ultra-secure password policies
- Set admin and user roles remotely
- Audit drives to see which files were added, removed, or changed

DataLocker Secure Drives - Encrypt data on a mobile drive and make sure nobody but the right people can access it.

Whether it's a small, highly-portable encrypted flash drive like the Sentry K300 or an ultra-secure, fast, and high-capacity drive like the DL4 FE, DataLocker secure drives offer powerful AES 256-bit encryption in an easy-to-use device. Everything a user needs to encrypt data is built right into a standalone data locker drive, and with SafeConsole, it's easy to remotely manage a whole fleet of DataLocker devices.

- Up to FIPS 140-2 Level 3 certification with AES 256-bit encryption
- Self-destruct after failed login attempts to prevent brute-force attacks
- Built-in McAfee antivirus scans added files (optional)
- Rapid crypto erase deletes all device data instantly
- Fully manageable via SafeConsole (select models)

PortBlocker - Ensure that users only use approved USB devices to prevent malware intrusion.

PortBlocker is a feature of SafeConsole that gives admins total endpoint port control to prevent data loss or intrusion. It allows them to whitelist only certain devices or fully lock down USB ports altogether, preventing users from introducing viruses by way of unsecured USB devices.

- Whitelist USB storage devices by Vendor ID, Product ID, or serial number
- Apply policies to groups of workstations or individual workstations
- Set USB ports to read-only mode to disable write capabilities on storage devices
- Automatically block devices when a workstation is used outside of a geolocation policy
- View all policy edits or changes in the SafeConsole audit logs

SafeCrypt - Encrypt any data stored on a workstation to lock up any sensitive data

SafeCrypt is a feature of SafeConsole that offers powerful encryption technology for data on desktops, laptops, and in the cloud. It allows users to create a secure virtual drive on their workstations. This folder works just like any other folder, but will encrypt any data added to it. This allows users to encrypt local files, network drives, external drives, and even single-user cloud storage.

- FIPS 140-2 certified
- Powerful AES 256-bit encryption
- Encrypt data on a local machine, store data anywhere
- Encrypted file names, read-only mode, file-type restrictions, and brute-force attack defense